#210 - Salt Typhoon and Vulnerable Telecoms

[00:00:00] **G Mark Hardy:** Hey, on today's CISO Tradecraft episode, we're going to take a look at a very fast moving event, something that you might've heard of called Salt Typhoon and the dangers of the issues that may present to you and your enterprise. So stick around. You're going to want to hear this episode.

Hello and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be more effective cybersecurity leader. My name is G Mark Hardy, and today I've got an episode for you that I think you're going to find very useful. I've got two experts on the line here from the Chertoff Group and we're going to go digging into what's going on now in terms of encryption with regard to enterprises. We're looking at our telecommunications infrastructure, potential foreign adversaries, and a whole lot more, but more importantly, what you can do about it. But before we get going with our show, a quick little note. Do zero day exploits and supply chain attacks keep you up at night? worry no more and harden your security with ThreatLocker. Worldwide companies trust ThreatLocker to secure their data and keep their businesses operations moving. ThreatLocker takes a deny by default approach to cybersecurity and provides a [00:01:00] full audit of every action, allowed or blocked, for risk management and compliance. Onboarding an operation is fully supported by their U. S. based CyberHero support team. Get a free 30 day trial now and see how ThreatLocker can help prevent ransomware and ensure compliance. Visit ThreatLocker. com. hey, back to the show. I'd like to introduce my special guest today. Adam Isles and Andreas Kurland, both from the Chertoff Group. Welcome to the show.

[00:01:26] **Adam Isles:** great to be here. It's great to

[00:01:27] **Andreas Kurland:** Thank you, G Mark.

[00:01:28] **G Mark Hardy:** And Adam, I think welcome back because I think we were featured on a show a while ago. And anyway, the reason I brought you and invited you to the show is that we had a fascinating discussion the other day about what's actually going on out there in terms of these issues I had mentioned. Salt typhoon, potential for federal government changing their stance on encryption, but you guys are the experts and this is your show.

So Adam, tell me what's going on?

[00:01:53] **Adam Isles:** let me put, things in context. And first of all, G Mark, you're the expert, too. So let's, we'll make this a conversation. [00:02:00] so we've heard a lot over the last week about a, threat actor campaign called, Salt Typhoon. Typhoon is the moniker that Microsoft and the U. S. government as well have assigned to Chinese, state actors.

And in 2024, we've seen a lot of references to various iterations of typhoons. We heard about Volt Typhoon in February, which was really a Chinese state threat actor campaign targeting critical infrastructure, more for strategic access than for accessing people's information. We heard about Flax Typhoon in early September, which was, around IoT, botnet campaigns.

And then we started hearing about Salt Typhoon, in September as well, and then the, idea that telecom sector had been, somehow penetrated was first reported, I think, in the Wall Street Journal in September. And there's been a flurry of activity this week, starting on Tuesday, December 3rd, where you had both, CISO and the FBI [00:03:00] saying, this compromise is ongoing.

It hasn't been eradicated yet. and actually for the first time, advising, citizens to use end to end encrypted, messaging and communication services. we saw on Wednesday, Ann Neuberger, the deputy national security advisor come out and confirm that, this, this, campaign has not been eradicated from at least eight, US telecoms providers. We saw joint guidance issued by CISA, FBI, NSA, the Australians, the Canadians, New Zealanders, really more focused on the telecom sector and how to better defend themselves. Interestingly, the Brits were not part of that for whatever reason, and we heard Jen Easterly also say that they're going to initiate a Cyber Safety Review Board review over this campaign.

On Thursday, the Federal Communications Commission, issued a proposed rulemaking that had two components to it. the first is what I [00:04:00] call the no duh rule, which, clarifies that, CALEA requires, telecom sector providers to secure the networks over which, law enforcement requests for information are being, are being requested.

And then there's also a proposal, for telecoms providers to, have, cyber risk reduction plans and, to, validate to test to compliance with those, plans. So we've seen a lot of activity this week, around this issue of, how secure are our core telecoms, internet service providers.

[00:04:37] **G Mark Hardy:** Now, it's rather interesting because as we look out there, we rely on our telecommunications providers as part of our core infrastructure. In fact, with a lot of the push toward MFA, most organizations have said we're totally relying upon the telephone networks to be around, to be able to either provide a push notification or SMS, but I do recommend the push notifications and being a little bit more secure. And for those who are totally paranoid people like me, [00:05:00] I'm using a YubiKey, but that's a distraction. More to the point, for CISOs and security leaders who are responsible for the security of their enterprise. And they're going to need to report back to their management when they read about this stuff in the Wall Street Journal and in Forbes and like to say, are we at risk? How do they answer that question? And what type of. background will they need to understand to be able to effectively evaluate the risks for their enterprise and then potentially move on to corrective actions.

[00:05:30] **Adam Isles:** I think I would start with looking ourselves in the mirror and saying, what's, our patient profile? And for everyone, basically identify three tiers of risk. there's a, baseline set of risks and we can think about risks in terms of potential impacts to confidentiality, integrity, and availability, right?

The classic CIA, framework for thinking about impacts from, cyber campaigns. in, in, in some respects, it's the, Particularly as we get [00:06:00] into heightened geopolitical risks, it's the integrity and availability issues that we start to worry about, which is, as we think back to volt typhoon, and, earlier campaigns, what is this access being used for?

But as we think about the nature of our business profile and we start to think about, do we actually, operate in China, or, Do we have sensitive IP? Are we defense contractors? are we, do we have a senior executive community that's active politically? now we start to worry, much more about confidentiality and, think about, and what this requires us, I think, to do is to say, Okay, like in real life, how do people communicate?

what are the modalities that we're using, to speak with each other? And I think we can start to break things down into, probably four basic categories. What are we doing from a messaging perspective? What are we doing from the point of view of voice [00:07:00] communications? What are we doing from the point of view of meeting over, virtual meeting platforms, this one?

And then, for emails and, other mechanisms, how are we communicating through those channels? We can start to think about each of those channels and

what optionality is, for, what baseline security looks like and how we can better secure those, our, use of those platforms.

[00:07:24] **G Mark Hardy:** Got that. Andreas, let's take a look. Let's start with messaging. Typically, people tend to live in some ecosystem. I have two phones that I travel with, like a residue from my government days, but also have private clients that I have, regular Android phone and a regular iPhone. And so never the two shall meet.

But that says I have to operate within two different ecosystems. Are there differences between them? I know that, for example, when somebody, I send a message to someone with an iPhone here from my Android phone and they go or whatever, I don't get a little smiley. I don't get a little thumbs up. I just get a little word saying somebody liked it or somebody did that.[00:08:00]

How different are these ecosystems? are there security risks when you transition from one to the other? And more importantly, are there security benefits from keeping your corporate communications within one of those ecosystems?

[00:08:12] **Andreas Kurland:** Yeah. so a lot to unpack there, G Mark. I would say that when we look at how messaging happens on in the Apple ecosystem and text messaging, it's iMessage. And when you go Apple to Apple, that's a fully encrypted, communication stream. And so that's offering, end to end security.

but that's not the case. Especially if you're going Apple to Android, unless you're using an end to end encryption platform like a Signal, a WhatsApp, or one of the other ones. I think sometimes there's a tendency for users to think that their data is secure. and they, their only person that's going to be seeing the information is the [00:09:00] recipient.

but, what we know is that, that's just not the case. the devil's always in the details. So when we look at these different ways people are communicating, text messaging, voice calls, virtual meetings, The actual solution being selected, has different, limiting factors. And so when we talk about messaging between Apple and Android, if you're doing it over signal.

That's end to end encrypted, but if you're just sending a regular text message, that's going to go over SMS and it's much more vulnerable to interception and to, the contents being displayed or available to someone who may be on that, telecommunications providers network.

[00:09:48] **Adam Isles:** We might just add a couple of points, which is, I think when we think about confidentiality risks, there are risks both to content and to metadata. and [00:10:00] Andreas, I'd add the metadata piece, which is to say, the other thing that we, and in fact, as we think about, Salt Typhoon, I think the, largest grab of information that's been publicly described so far has actually been around metadata.

It's been around call detail records, who was calling whom when, who was texting whom when. And so we certainly have to think about whether we're concerned about that metadata being available. to, to our adversaries on the one hand, on the other hand, we also need to think, G Mark, this was actually, I think, a point you were making when we were chatting yesterday about, if we're going to use one of these other platforms, we're also essentially providing those platforms metadata about ourselves.

Are we, dumping our entire contact list into, WhatsApp? And so we just need to be, eyes wide open about the fact that, we may be doing that.

[00:10:56] **G Mark Hardy:** And that's a good insight on that because what we look at is using an [00:11:00] analogy of DNS and virtual private networks. So we go back to the pre Snowden days where most things were HTTP. I can remember at DEF CON where they had the wall of shame. There's a wall of sheep, I'm sorry, which it should have been a wall of shame for everybody who is logging in with an unsecured connection.

And you would see these user IDs and asterisked out passwords, but the first visibles, you had, and we're just scrolling a mile a minute. And this is at a hacker conference. You'd think they'd know better, but most resources weren't out there today. Click. Click. It had to change your business model because everything has gone encrypted.

That said, what you mentioned is very important about metadata. And for example, if I log in to a hotel because I'm on travel and I'm doing my HTTPS, sure, my communications are secured by TLS and I've got a key exchange that's taking place, but every website I got to, everything that you see in the URL can potentially be visible to the third party.

Now, the question is, Whom do you trust? Do I trust the hotel? Do I trust the ISP? Do I trust my VPN provider? At some point, somebody needs to [00:12:00] be able to read the address on that digital envelope to know how to deliver the mail, and it's just a matter of what postal service do you trust. Here we're looking at the large scale accumulation of metadata, and so we say, for

example, if you're doing an investigation, let's say law enforcement, we have a suspect up in New York who's suspected of killing somebody up there and they're on the run from the lung.

They'd sure love to know, can we get the information on geolocating this? Who's this person talking to? Who'd they last text? Who might they have communicated with? let's take that as a corporate level. And an enterprise level. And we kick that up a little bit higher and say, okay, as a CISO, what types of information is my organization doing?

Do I have FINRA compliance requirements that I need to meet? And as a result, some of this information where I'm working on the deal, that if it gets out, could allow somebody to materially, benefit from it by making some trades based upon what would be insider information. But for organizations that don't have that insider risk, but if you do R& D, if we're doing acquisitions, M& A, there's a whole bunch [00:13:00] of things that we really just don't want to get out there.

So how do we help people understand Okay, everything's encrypted. My boss says we're fine, but that metadata really has a tremendous amount of value. How do we articulate that to executives so that the aha moment comes and they get it and they get the risk?

[00:13:16] **Adam Isles:** Well I think the question is, who might have access to the metadata? And, we're in the circumstance, where, there's a risk about, a Chinese adversary having access to the metadata. and, what's our alternative. Our alternative is to basically use platforms like Signal, and WhatsApp, to be able to communicate, text messaging.

and the only thing, I think the only point there is, We're in a risk management, not a risk elimination business. And so there's just, an issue of, our, now we've got another provider, instead of Verizon or AT& [00:14:00] T, it's, it's Meta or Signal, that has access to our metadata.

And we just want to go into that, eyes wide open.

[00:14:07] **G Mark Hardy:** Looking at Salt Typhoon and what we know, at least at the unclass level, are we more likely to have less loss of information going to a platform like Signal than just allowing SMS? Do we assume that the Verizon and T Mobile and all of the AT& T's are wholly owned and compromised by an adversary?

What's, a proper risk profile to take right here with incomplete information?

[00:14:31] **Adam Isles:** G Mark, what do you think on that?

[00:14:34] **G Mark Hardy:** my thought is this, is that if you take a look at some of these encrypted messaging communications, they've come a long way. It used to be that WhatsApp was very popular. In fact, when I get on my Southwest Airlines, I don't even have to pay the $8 to use WhatsApp. That's one of the free messaging.

They allow me to do that and Apple messaging, but I can't do SMS. And there's probably a good reason for that, maybe from a revenue perspective. But in addition to not being able to use SMS, I can't do things like RCS, Rich Communication Service, which is going to allow me to [00:15:00] do cross platform. And so what I recommend for enterprise CISOs is to go ahead and have a plan that allows you to go ahead, assess your risk.

Are you concerned about confidentiality? What about integrity? Is it possible for SMS to be changed in route if they're in unencrypted and they're in that same site? Probably. And then the availability of the system, which is typically what we look at, but take for granted. Oh yeah, Verizon is always going to be there.

T Mobile is always going to be there until they're not. Which is one of the things that I recommend in terms of setting up things for MFA is you need to have one other way for an administrator to get in if your telecommunications network goes down. If you're totally dependent on the communications network and that goes down, you're locked out. So back to the question at hand, what do I recommend? When you create a directory of contacts in a cell phone. And for example, here on my iPhone, I have all the people that I can talk to. And I had to reveal that, which then can use as a telephone call. I could use that as a message. And when [00:16:00] they fire up something like a signal or a WhatsApp or a telegram, et cetera, do you want to import your contacts?

One of the first questions they ask, if you say yes, You've just simply exposed every single one of your contacts, relevant or not, to that third party provider. What is it that we want to do? We want to be able to tell our organizations that our intra organizational communications are secure from compromise and from loss of integrity. In doing so, the availability suggests that we go with a Well known provider. It's not Joe's Delicatessen and Secure Messaging Service. And we have some excellent choices out there. Signal, in my opinion, would be the one I would recommend. It's what I use, but I also run WhatsApp. I also run

Telegram. I run a few others based upon the needs of my clients and other communications experts.

But if you as a CISO can drive that, drive everybody on the same platform, as you had indicated earlier, the problem is at the seams, at the [00:17:00] edges. If I'm all within the Apple ecosystem, I'm fine. If I'm over here, perhaps in the Android system, I may be fine. But as soon as I do this cross border, something has to get decrypted out of this ecosystem to encrypt into that ecosystem, and that's the weakness.

And that weakness occurs not at your endpoint, not at some place where somebody can alligator clip into your telephone, but it's going to be at the service provider level and our adversaries know that. And so that's the targeting that I think that we've been seeing from some of these releases that have come out of the federal government just in the last few days to say, yeah, we're worried about this and you should be worried about it too.

[00:17:36] **Adam Isles:** I'm going to make another point about messaging for a moment, and I'm going to pick up on a point that you made earlier. messaging, SMS text messaging has been used for, the conveyance of one-time Passcodes. as, we push everyone to multifactor authentication, we see a number of apps still using, one-time Passcodes.

and, [00:18:00] this is another area where we wanna really drive people off. SMS, one-time passcode based, multifactor into. the authenticators, the duos, the octas, of the world. and, the reason for that, is, what you talked about earlier, the potential to compromise the integrity, of, or, the confidentiality of those communications.

SIM swapping has been, a risk for, years, and, what I would also say is in that, All of the attention around Assault Typhoon over this last week, and what the government has, what the telecommunications providers have or haven't been able to do. the Department of Justice also unsealed a criminal complaint against a member of Scattered Spider.

and what that complaint alleged is that, that individual, had been able to gain access inside a telecommunications provider, for, for criminal purposes. [00:19:00] and, and so you, and, by the way, they didn't allege SIM swapping on his part, except that they alleged he'd been a long time SIM swapping expert earlier in his, in his life.

So we also, as we're thinking about that channel, that messaging channel and the risks associated with it, We want to get authentication off that channel into, a, a, stronger form of a multifactor, whether it's, you talked about Yubikey earlier, number matching, but, app based authentication and, ideally hardware based, certificate based, authentication in, in, in terms of multifactor.

So I just as we're thinking about. why are we using message messaging? I did want to also think about that. very important, use case,

[00:19:49] **G Mark Hardy:** okay, so we've talked a lot about texting, but the indication that you gave us earlier, there's four different levels we need to be worried about. We're talking about messaging, voice, being able to do [00:20:00] meetings like we're doing right now, and then ultimately an email. So let's move on to the question about voice. Are there any concerns with that? If we go back to the old days where we watched the old mob movies where the FBI is sitting there with a couple alligator clips in the basement and they've got the headset on, and then the bad guys have the wives talk about something so that they realize, hey, this is not a monitorable conversation. FBI has to get off the line and then the mob guys talk about their stuff. Okay. So that's the stuff of Hollywood movies and things today. And for the most part, landlines are pretty much gone. But what's the concern now in the digital world with regard to landlines? And here's the confidentiality, integrity, availability, and specifically, does it relate to any of these typhoon issues?

[00:20:39] **Adam Isles:** Yeah. So from the Typhoon perspective, we've got a confidentiality issue and there is some suggestion that while Most of the compromised information in Salt Typhoon was around metadata, that there were certain use cases where communications content itself, was also compromised. and you've got an [00:21:00] telecommunications environment, even assuming, we're, we've moved beyond, wireclips and landlines.

you still have a, a mess of routers and switches, a variety of equipment, in, inside, all of these networks, that is, if you've got, kind of God level access to them, I think, potentially at risk. Andreas, I don't know if you want to cover, what, what some alternative options are for, voice communications.

[00:21:29] **Andreas Kurland:** Yeah. so with voice, similar to, text messaging, the vulnerability is going to be on the service provider side. your call over cell phone towers, between your device and the cell tower may be encrypted, may be secured, but once it gets to that internal telco system, that's where, this data is more exposed.

and so again, it goes back to that end to end encryption. [00:22:00] and when you look at, FaceTime, Signal, WhatsApp, they're providing that full kind of tunnel from your device to the recipient's device. and so if any of that network traffic, that data is intercepted at any point, between you and the service provider, the, across the internet, it's simply, encrypted data and nothing can be done with it.

I think that's really The big takeaway is that, because we've seen Salt Typhoon and, other, excursions into these big telco and ISP service providers, you can't trust that your data is going to be secure on those systems. And so trying to control end to end, I think is really a key.

[00:22:52] **G Mark Hardy:** So voice communications, then we're saying, Again, that's probably the one that executives that are non technical are going to stand a lot [00:23:00] more. They pick up the phone, buy, sell, do whatever it is. And they want to make sure that those are secure. We tend not to worry too much about integrity in the past because for the most part, voice is going to be voice.

And it's not like it's a store and forward where I could take it offline and change it. Of course. And then the whole question about deep fakes is a tangent in a different direction, but integrity that we're talking about. I'm not gonna get into in this particular show because we're looking at what's going on and what are some of the concerns here with regard to voice, but does it make sense then to say, if I'm going from a. Apple iPhone to an Apple iPhone, or a type of a call that's coming over a different ecosystem, or even if I'm using a SIP based telephone that's on my desk that I pick up, and as you pointed out, that SIP protocol has to get figured out somewhere, and until it goes off to the telecom provider, any access to that network cabinet gives you potential access to that communications and that traffic. But again, We're [00:24:00] looking at this at a grand scale, at a level where federal law enforcement has done sort of a 180 where instead of saying, yeah, at an enterprise level, you don't really need this encryption. They're saying, yeah, we think we do. And some people are saying, Hey, we've been gaslighted all this time.

And all of a sudden the federal government who likes to be able to listen in on stuff is suddenly realizing, Hey, it's better to keep everything secure than it is to allow us that access. It's starting to sound like it's getting a lot more severe. then some of that initial press releases that are coming out. So the two questions I think I'm putting on the table are, from a voice perspective, what are prescriptive approaches that we can say to help tighten up communications for an enterprise level? And then the second one is, from the perspective of a

change or a sea change in the messaging that we're hearing from the government, what is it that we can potentially learn from this?

[00:24:54] **Adam Isles:** do think we need to think from an enterprise level about, the extent to which we're talking about [00:25:00] communications within the enterprise, from Andreas to me, to you, versus, communications, outside the enterprise. And so in the former case, if we're standardizing our, our voice hardware, say on Apple, we've got the ability to use FaceTime, or FaceTime audio, for, any sensitive communications.

Now, security not just needs to be, risk based and assured, it needs to be intuitive. and so there's a huge training component, that goes along with this as well. So are we saying thou shalt only use, FaceTime audio ever for calls? Not necessarily, but we are trying to train people on, what calls, would tend to be more sensitive?

How do you use judgment on that? And, frankly, is it really that much more difficult to use, FaceTime audio, for, a call [00:26:00] versus. just, dialing the number. So we think about that, there's probably more complexity once we're, moving outside the organization and we're talking about talking to external stakeholders.

I think part of this gets to a question around, as a community, how do we see higher levels of adoption of, whatever the platform is? the advantage of a, signal. over WhatsApp is that it can operate across platform, right? we can bring in Android users, Apple users, and, those technologies will work across platforms.

[00:26:34] **G Mark Hardy:** Andreas, thoughts about this seat change, if you will, of what we're hearing from Washington and Law Enforcement. Is it a seat change or is it just a messaging that we just haven't picked up on before that now we're finally getting?

[00:26:47] **Andreas Kurland:** Yeah, it's a great point, G Mark. and it's interesting that the guidance from the FBI and CISA that came out this past week was not official guidance. It was not an official alert, saying, hey, everyone do [00:27:00] this. it was senior officials from the FBI and CISA, recommending Americans switch to encrypted messaging apps.

but it does portend to a change of, perspective, and also to the seriousness of, what the FBI and CISA are seeing with this SALT typhoon hack. and I think that's why the Cyber Safety Review Board, looking into this, Seeing what they

find when that report comes out in a number of months is going to be very interesting, because, like we've seen with previous, intrusions, the Microsoft, from 2023, where Cyber Safety Review Board looked into that and Lapsus in 2022, those are always very illuminating and really get to the details of, how the threat actor, Got in, what the vulnerabilities were and how things needed to change, in order to prevent that in the future.

So [00:28:00] I think, it is interesting that we're hearing from the U S government, at different levels, Hey, encryption is our friend and you should use strong encryption and to end encryption. I think it does show that there is concern about, You can't just trust that service providers, regardless of who they are, are going to secure the data.

You want to put your trust in strong encryption.

[00:28:29] **G Mark Hardy:** So we've talked about messaging. We've talked about voice. Let's talk about meetings. So we're in a meeting right now. As you're recording this, we're using a special tool. But if you recall, during lockdown, there was this big, huge push to Zoom. Stock price went through the roof, but also things like Zoom bombings take place where they would have a call and all of a sudden somebody's in the call that's not supposed to be there.

That had nothing to do with encryption. Just had to do really with access controls and managing that. Any suggestions that you have to help organizations at the enterprise level Direct all of their meeting communications into [00:29:00] any particular platform. Do you see any risks with any of those? And in general, unlike messaging or even voice, I don't see a cross platform capability that exists today.

I can't say, Oh, I want to come in on Zoom. You come in on Teams and we'll talk together. It's no, it's my island or your island. What do we recommend?

[00:29:20] **Andreas Kurland:** that, that's a great point. I think when you look at the kind of most common platforms for virtual meetings, whether it's Zoom, WebEx, Teams, Google Meet, they all are handling You know, the security and the privacy of those interactions in different ways. a lot of these platforms will fully encrypt end to end one to one calls.

but once you have group calls, it's no longer end to end encrypted. And a reason for that is because on the service provider side, for them to offer certain functionality like cloud recording, live transcription, That requires being able to process the data in [00:30:00] real time as that meeting is occurring.

And there are platforms, Zoom is one of them. If it's configured specifically, for end to end encryption for group meetings, it, it does that. The trade off is that you're losing some of that functionality. so it's always a give and take and it probably goes back to, what information is being communicated and what's the sensitivity and what's the risk tolerance of the organization and the participants.

I don't think anyone is saying you need to have full end to end encryption of every way you communicate all the time. It's just understanding. if we've settled on WebEx or Teams or whatever platform, we, as an organization need to understand what the risks are and what the, security and privacy controls are within that platform and make sure it aligns with our risk tolerance.

[00:30:56] **Adam Isles:** I think this is where, some of the secure by design conversation comes in as [00:31:00] well. And so part of what we're thinking about from a kind of a supplier due diligence perspective, as we're thinking about different optionality and platforms is what do we know about application hardening, application security features, what the default is.

And I'll just take those in reverse order. Andreas, what you said. You know about Zoom and I think of all the major platforms, zoom is the one that operates, that, that offers, end, encryption for, group virtual meetings is that's not by default, which is fine. We just need to understand what functionality is, implemented or not implemented, by default.

but the point is from an application security feature, it's there. not all platforms I, are going to offer as a security feature, group, end to end encryption. And then from an application hardening perspective, this is where, we get into a little bit of a broader conversation, particularly as we start looking at, a more diverse [00:32:00] ecosystem of, Okay.

So like exactly how well was, the source code, you used to produce this application, secured, what kind of testing you need to do? What did you do on source code management? how was the source code library hardened? And, what do we know about the R& D teams that were doing that work?

And I say this, not because this is a theoretical concern, but we saw, last year we saw the North Koreans. successfully use a, actually a double supply chain hack to get inside a company called 3CX, right? Which, produces video conferencing software. So we do want to think a little bit about, what do we know about the security of not just product and deployment, but product and development, for these technologies we use.

And oh, by the way, we want to make sure that we're, updating our own operating systems on our iPhones and our Androids, as [00:33:00] well.

[00:33:01] **Andreas Kurland:** Yeah. And I would just add Adam, talking about within your own organization, how you control, how people are communicating, it's that deliberate look at for virtual meetings. This is our platform. We understand how it needs to be configured to be secure. and then ensuring that people try to have some technical controls in place to ensure people are not using unapproved or, less reliable forms of communication that there's been many incidents of, threat actors putting out, teleconference and virtual meeting software.

that, is, are laden with info stealers and is providing, leaking information, and so you can't, that kind of goes back to the training and awareness aspect where you have to settle on here's what we're using and then make sure your people understand the risks of, [00:34:00] going outside that ecosystem.

And ideally you have the controls in place to prevent that.

[00:34:07] **G Mark Hardy:** So we talked about being able to look at the meeting and some of the ideas that, for example, as you said, within Zoom, if the meeting organizer allows for it, you can have up to 200 people in an encrypted session, but most of the other things that are out there in terms of stuff like WebEx, GoToMeeting, Google Meet, Teams, etc.

will encrypt your data in transit. But as you said, it's not really end to end encrypted. It doesn't, it has to decrypt somewhere. So that you can even apply some intelligence on that. And as we get on to the fourth element, we want to talk about email. Of course, we look at things, for example, I have a Gmail account.

I've had it since 2007 or six. I've been one of the early adopters as I tend to be on a lot of technology. And if you use a web based interface, you're always getting context sensitive ads based upon it reading your email. And you have to know all that calculation is not taking place on my Desktop, that's somewhere upstream.

So as we think about a store and forward network, like email, I create an [00:35:00] email, if it's encrypted, and it goes encrypted up to the server, and my recipient gets encrypted down from the server, and maybe we're in the same tenant in Microsoft, so we're going to say, hey, is that Microsoft fully completed? Or at some point, is there a break in there where, again, we're not

worried about average class hacker or a cracker or somebody operating at that level, but we're talking about state level actors being able to access infrastructures.

Where do those seams exist for exposure and how can we as chief information security officers and security leaders alter or try to push for alterations of our strategy? to reduce that risk as much as possible.

So for example at the Pentagon what would happen is we would have everybody in a global address list, a GAL. And when I could go ahead and I could able encryption. And you can also sign up, but let's talk about enabling the encryption. Click that little red icon up there in Outlook. And then it would go encrypted all the way through to my recipients, at which point it was then decrypted [00:36:00] because we had a public key infrastructure that was set up so that we had a couple million keys that were in there.

But when I went to the Army War College, it turned out that my Navy cert didn't work with the Army. I think it had something to do with football games and they just didn't want to play well with each other. This has fixed that subsequently. But back to the idea of being able to have everybody in that same ecosystem, If I forwarded that email to somebody, a third party contractor, for example, who was not in the global address list, that message then showed up as a P7S attachment.

And you couldn't open it because, you didn't have one of the keys that were allowed into it. So it seems that there's two issues here. One is, can we enable encryption within the enterprise? And the answer seems to be yes, even if it's a huge enterprise like DoD. But then how do you deal with the issue of secure email communications across organizations.

And can that really be done? Or do we have to first encrypt our little message locally, send it as a blob, decrypt it on the other end? Because the thing with store and forward is it's going to [00:37:00] exist and maybe persist in more than one location, whether you like it or not.

[00:37:06] **Andreas Kurland:** Yeah. I meann so when you look at how email is sent and, the security of email, You can encrypt email with Gmail with Outlook through Microsoft M365. the issue is that those messages are going, from your device to many different intermediary devices. And for, spam filtering and, malicious content filtering.

That content is decrypted as Microsoft or Google or whoever is handling it and then doing the re encryption and sending it to the end user. So again, the threat or the risk is that if, that service provider, that intermediary, if there's a malicious presence or an insider or a breach, on their network or with their [00:38:00] systems, your information is, even though you're, you sent an encrypted email, it's not truly end to end encrypted.

there are services, that do full end to end encryption. You can also roll out with Outlook, and other mail clients, SMIME, that PKI infrastructure. The problem is, the larger the organization, the more kind of overhead there is to set that up, to maintain it, to get the certificates loaded on everyone's end device and replace them when they expire.

and email encryption is not necessarily the, simplest, thing to maintain long term. but, services like ProtonMail, they do offer end to end encryption, where ProtonMail is not, is, and no one in between has ever seen kind of the contents.

of that message

[00:38:58] **Adam Isles:** we think about [00:39:00] end to end encrypted emails, From a CISO's perspective, I think, again, we're trying to train on use cases. So are we telling the organization to try and, wholesale adopt end to end encryption for everything that gets sent out? Not necessarily, but if we're a bank, we are thinking about, are we using, Virtru for if we've got sensitive financial information, account numbers, social security numbers, things that could be used to open a bank account or, provide insights into, what someone's balances are.

Like we very much do want to be thinking about, using these tools, in those use cases where a bank is interacting with its customer or, a mortgage service provider or someone like that.

[00:39:47] **Andreas Kurland:** Yeah, I would certainly agree that, just because you have a tool doesn't mean that's the best tool for in every situation. And there's many ways to securely [00:40:00] share documents without emailing them. and so that it may not be, let's send this through email and let's try to make sure it's encrypted end to end.

Maybe it's, let's put it in this secure document repository and provide access for a limited amount of time to these specific users. and again, it's,

[00:40:20] **Adam Isles:** That's a great point, right? When we're thinking about documents, attachments, oh, by the way, if they're in an email, Depending on their size, they may be going through a content distribution network as well, just based on we're in the cloud, large volume. So we, for sure, from a training point of view, want to be pointing people towards, SharePoint, or, Box or whatever it is, versus, versus email.

[00:40:47] **G Mark Hardy:** And then you email the link, and then that service, whether it's SharePoint or Box, controls the access, and sorry, you don't have the right link, you're not the right authentication, and we basically are then able to keep that down. an interceptor would know, A, [00:41:00] you sent a link to something, But they're not going to be able to get that, which is a brilliant insight and things like that.

[00:41:05] **Adam Isles:** We're going to come back to secure by design again on the, the, file shares, right? Cause we want to make sure that those companies, are, taking security seriously. and, are, particularly testing anything that's internet facing, but yes, that's the general direction we want to head.

[00:41:23] **G Mark Hardy:** let's go ahead and wrap up here because we're getting close to the end of our show. So we've looked at what the risk is out there. There's been some announcements recently from the federal government looking at salt typhoon and the possibility of our infrastructures or telecommunications infrastructure, having been infiltrated by a nation states intelligence services.

Big concern there. And those outside who aren't operating those telecommunication services, but rely upon them, have to look at different levels of communications for our enterprises. We have to worry about messaging, worrying about voice, worrying about meetings and worrying about email. And we've discussed in this episode, some of your recommendations for how we can go ahead and mitigate that risk for enterprise, [00:42:00] communicate that information to our decision making executives so they better understand what that risk is, and then can either go ahead and fund or approve those types of initiatives going forward.

Now you guys at the Chertoff Group have some very impressive clients that you do a lot of work for. And if someone says, Hey, you guys might be able to help us too, because, this is an issue and we may or may not have the resources, the insight. How does someone get in touch with you? And then how would they go ahead and get some more information as to how to proceed?

[00:42:28] **Adam Isles:** you can reach us through, info@ChertoffGroup.Com. and, you can, I'm adam.isles@ChertoffGroup.Com. we'd, we'd love to have a conversation with, with, folks that need help in this space. at the end of the day, I think what we're You know, what we're, trying to do is to create a balance with security that's risk based, trusted, and intuitive.

So the risk based piece is, do we understand from a, [00:43:00] again, from a threat vulnerability and consequence perspective, on the consequence side, what's the sensitivity information we're dealing with? And do we want to apply different solutions towards different levels of sensitivity? from the assurance point of view, this comes back to the secure by design, understanding there's no such thing as risk elimination.

These different platforms, what do we understand about application hardening, good application security features, what the defaults are, and then the intuitive piece, I think, in some ways for CISO is, is the most challenging, which is, What's going to work with our user base? What's a, a reasonable human being going to be able to easily adopt into business as usual, such that you don't have people doing end runs around the solutions that you're, You're providing

[00:43:53] **G Mark Hardy:** Andreas, any final thoughts?

[00:43:54] **Andreas Kurland:** I, I would just say, that's a great point, Adam, about the usability. So it's [00:44:00] great to design systems that are highly secure. but if they don't meet the business's kind of internal processes and norms and, how people are used to interacting or understand how they need to interact, then users will do end arounds.

and so it's being deliberate about here's our risk profile, here's our tolerance, here's the solutions that are going to work to address and reduce that risk measurably. And then we're going to be socializing that and ensuring that our users understand what the expectations are and, how to, do their jobs in a safe and secure manner.

So I think that is, a good takeaway.

[00:44:44] **G Mark Hardy:** Thank you, Adam Miles and Andreas Kurland from the Chertoff Group. You've provided us some excellent insights on some of what the risk is, the issue that's going on. And thank you for the information to be able to go ahead for those who want to follow up to get access to your resources. Again, [00:45:00] info@chertoffgroup.Com. It'll also be in the show notes along with some of the references that we've talked about in the show. If

you like this show, go ahead and please subscribe if you're not doing so already. We're on LinkedIn. We have over 33, 000 subscribers there and you'd like to follow us there, but we also have a Substack newsletter.

We're on YouTube. Make sure you like us or give us a five star so you can help us get the word out to improve others tradecraft from your knowledge of CISO Tradecraft. So this is your host, G Mark Hardy. Thank you for listening in. Until next time, stay safe out there.